WORKSHEET #10 – MATH 5405
SPRING 2016

DUE THURSDAY, MARCH 31ST

More fun with elliptic curves. We begin with a degenerate elliptic curve.

1. Let $P = (1, 1)$ be a point on $y^2 = x^3$. Compute nP for $n = 1, 2, 3, 4, 5$. Can you guess what nP is? At the very least, if $nP = (x_n, y_n)$, what is x_n/y_n?

2. Let $P = (2, 3)$ be a point on the elliptic curve $y^2 = x^3 - 10x + 21$ modulo 557. Show that $189P = O$ but $63P \neq O$ and $27P \neq O$.

Hint: This looks bad. But remember, you can compute $2P, 4P, 8P$, etc. rather easily. Thus derive point addition and doubling formula to help with your work. Of course, use a phone / calculator / computer to assist with the modular arithmetic, finding inverses mod 557, etc.